

FIG. 1

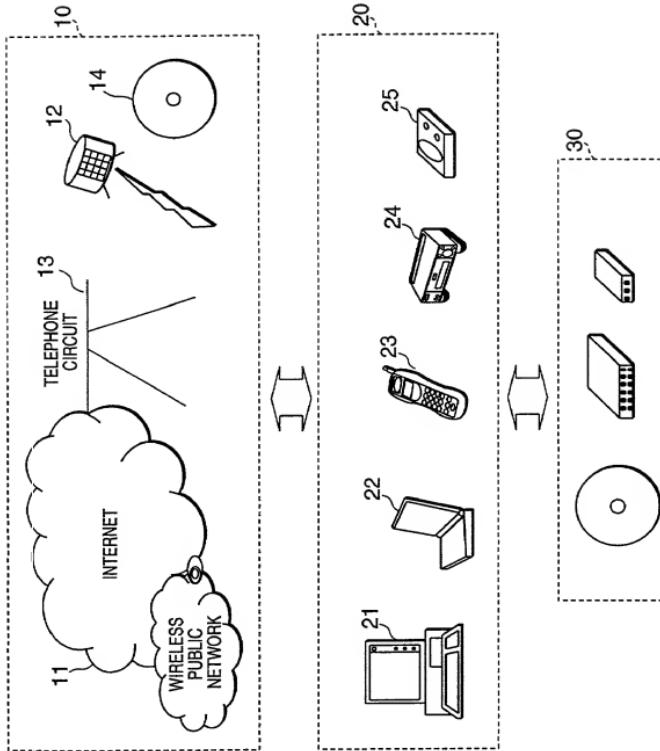


FIG. 2

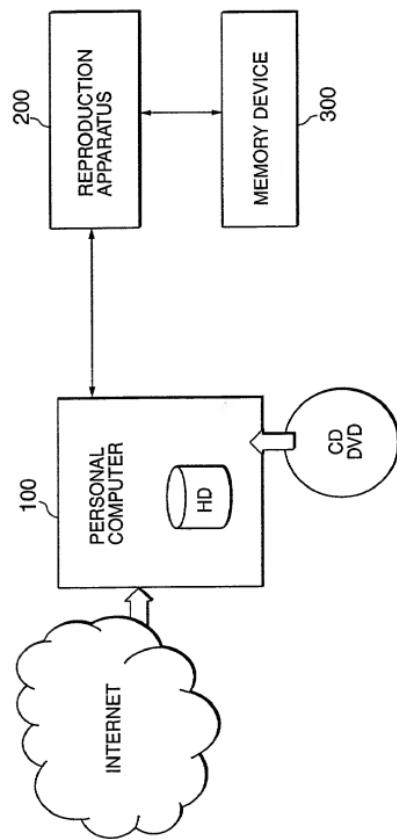


FIG. 3

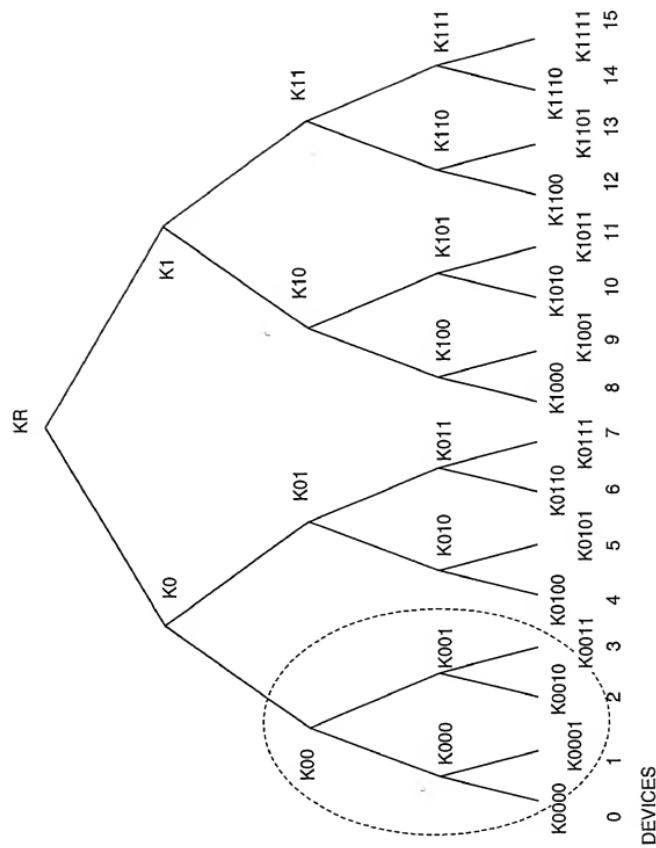


FIG. 4

EKB (ENABLING KEY BLOCK) EXAMPLE 1
DELIVERS NODE KEYS OF VERSION (t) TO DEVICES 0, 1, AND 2

(A)

VERSION : t	
INDEX	ENCIPHERING KEY
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

EKB (ENABLING KEY BLOCK) EXAMPLE 2
DELIVER NODE KEY OF VERSION (t) TO DEVICES 0, 1, AND 2

(B)

VERSION : t	
INDEX	ENCIPHERING KEY
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG. 5

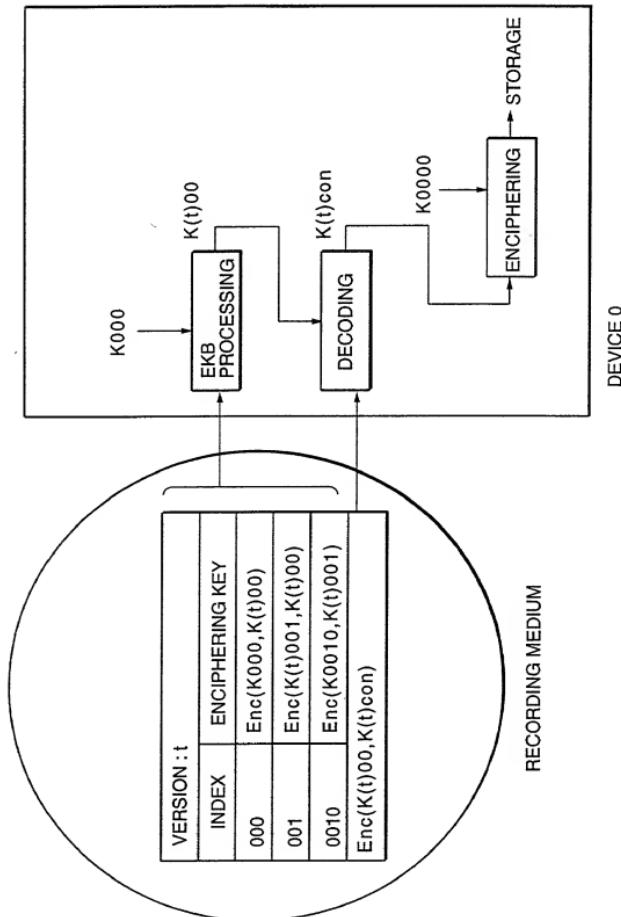


FIG. 6

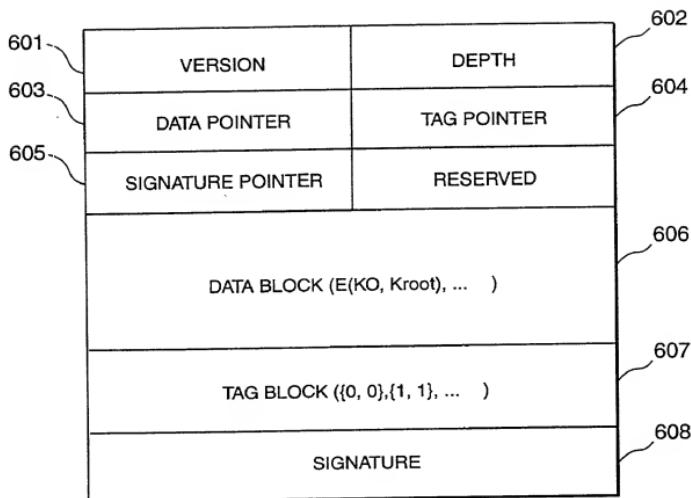


FIG. 7

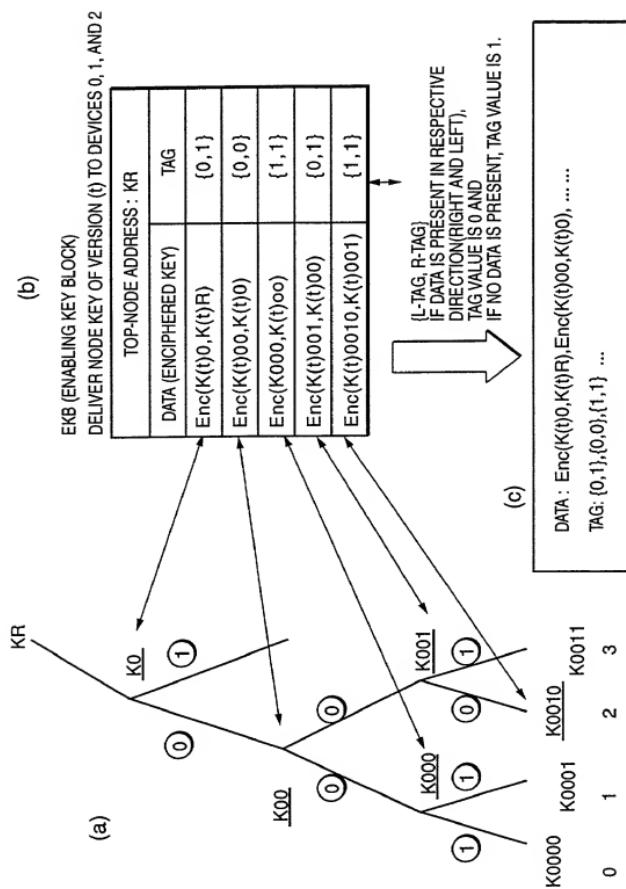


FIG. 8

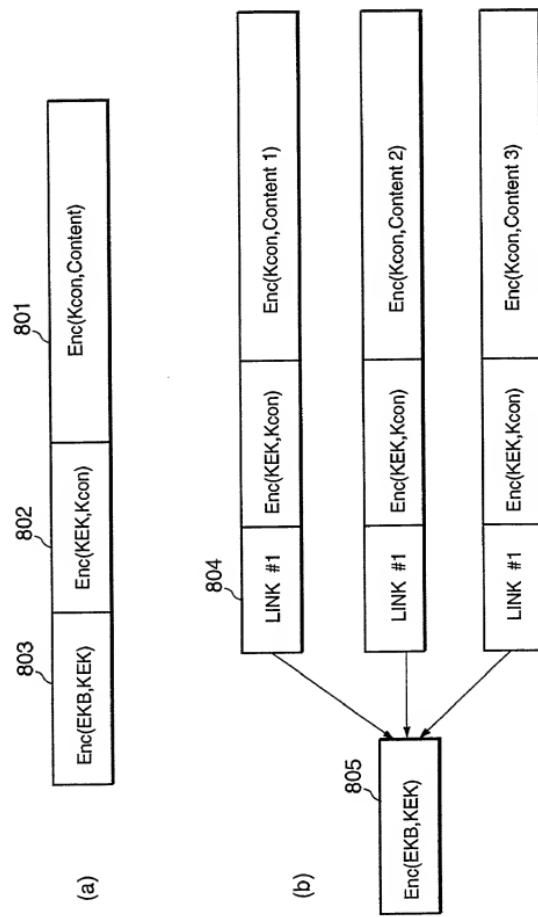


FIG. 9

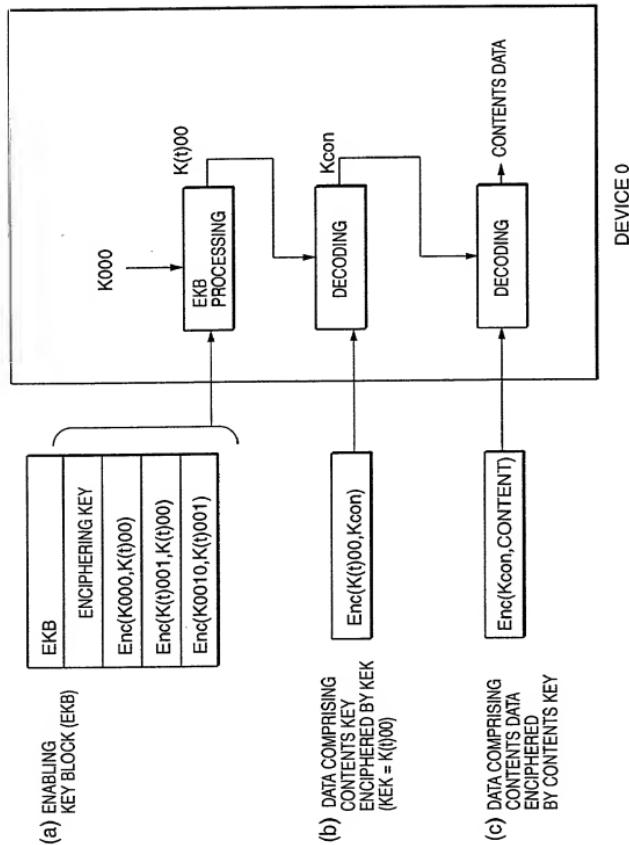


FIG. 10

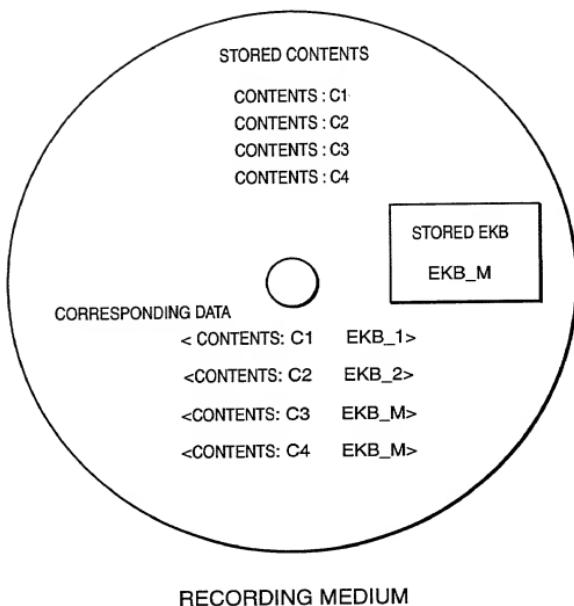


FIG. 11

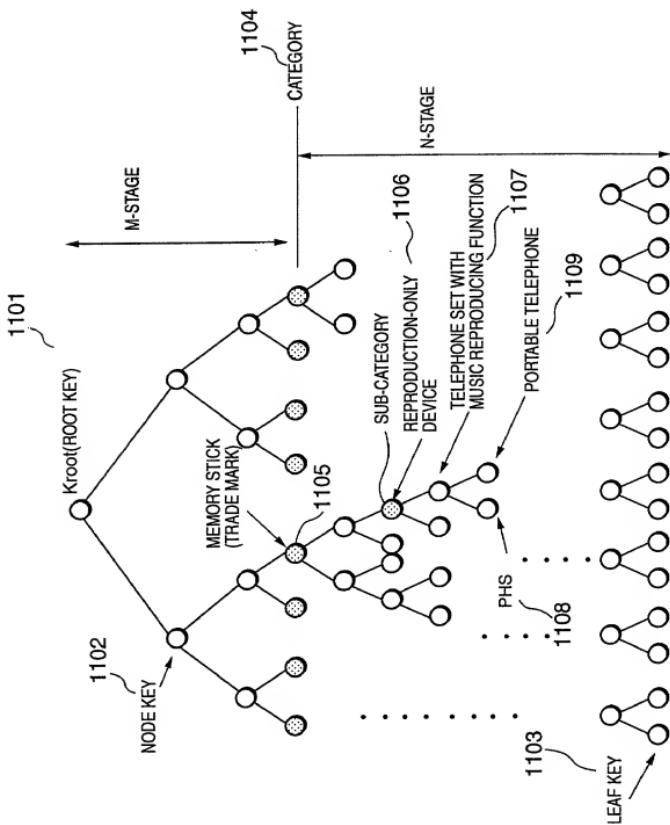
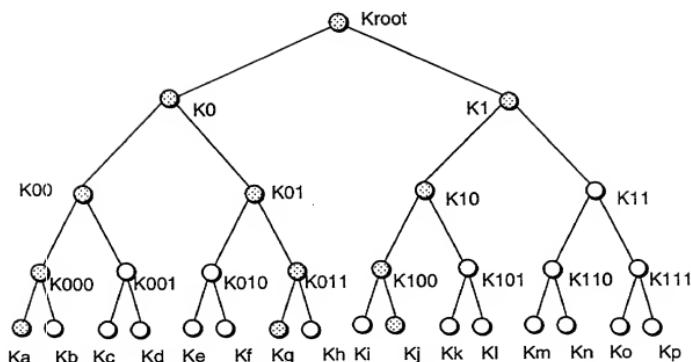


FIG. 12

(a)



(b)

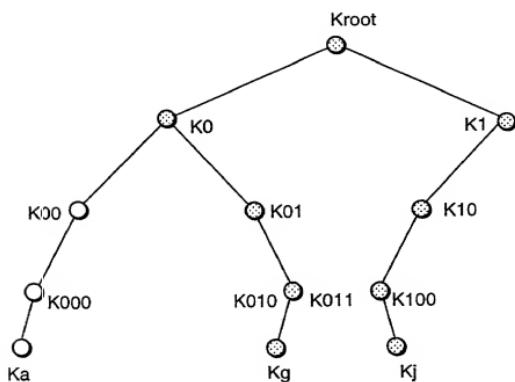


FIG. 13

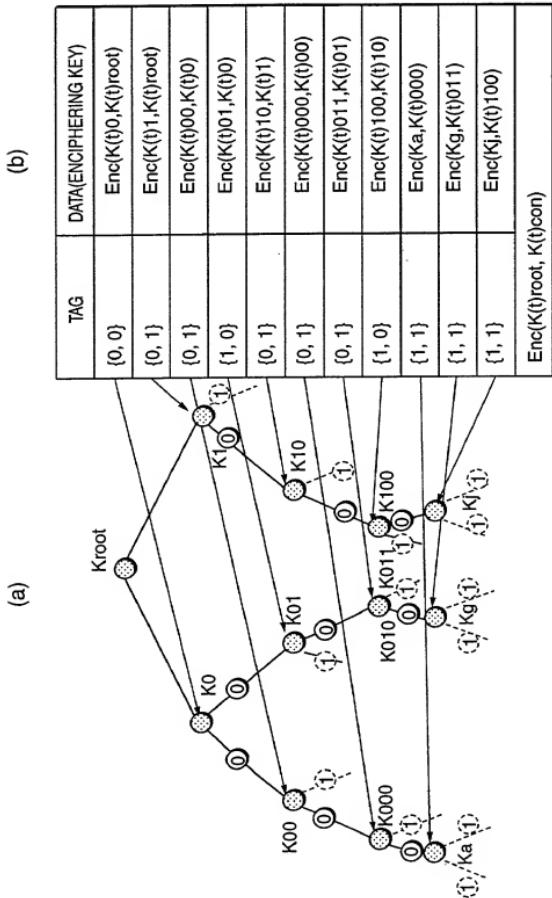


FIG. 14

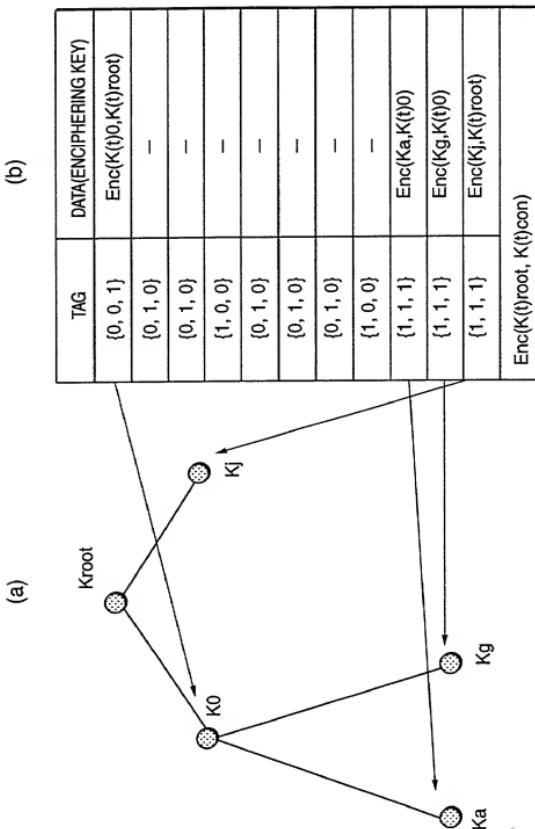


FIG. 15

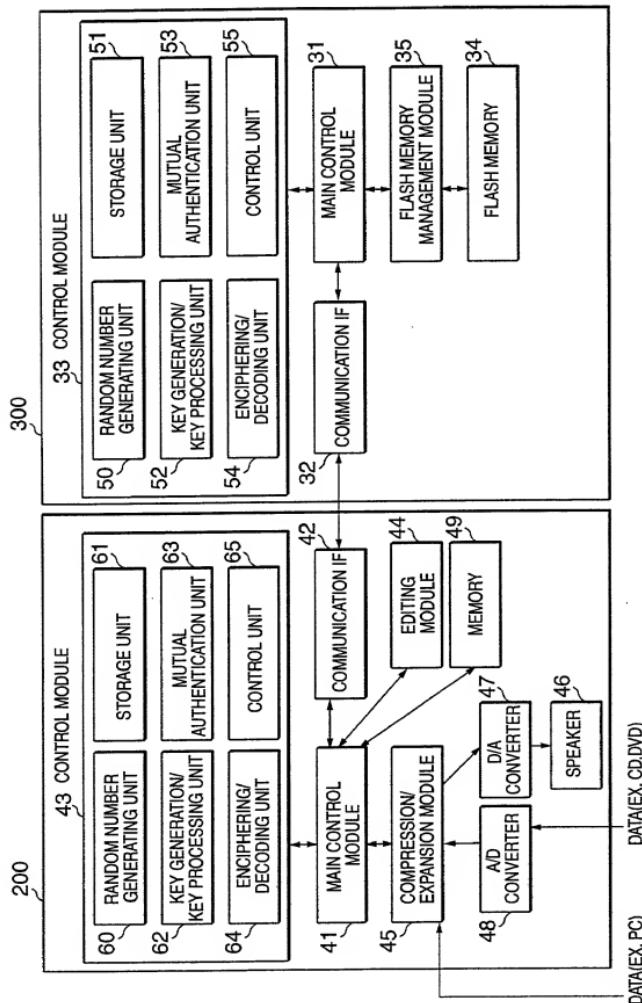


FIG. 16

DATA STORED IN A STORAGE UNIT OF A MEMORY DEVICE

AUTHENTICATION KEY DATA	IK0 IK1 IK2 IK3 : : IK30 IK31
DEVICE IDENTIFICATION DATA	ID0
STORAGE KEY DATA	Kstm

FIG. 17

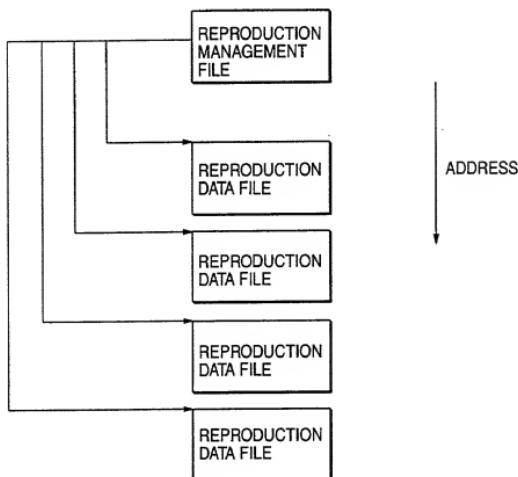


FIG. 18

REPRODUCTION MANAGEMENT FILE

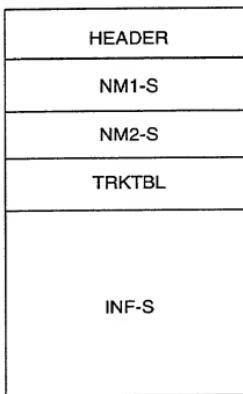


FIG. 19

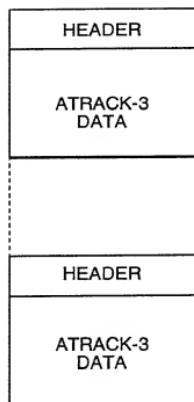
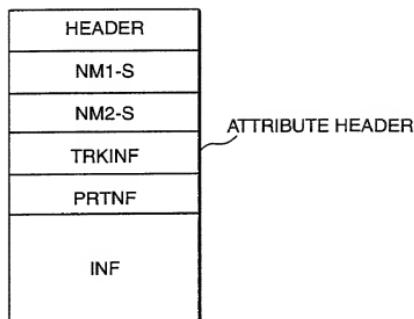


FIG. 20

REPRODUCTION MANAGEMENT FILE

A

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID-TLO	RESERVED		MCODE		REVISION					RESERVED					
0x0010	SN1C+L	SN2C+L	SINF SIZE	T-TRK	VerNo.						RESERVED					

B

0x0020	NM1-S(256)																												
0x0120	NM2-S(512)																												
0x0310																													
0x0320	RESERVED(4)	EKB VERSION				E(Kstm,Kcon)																							
0x0330	E(KEKn,Kcon)																												
0x0340	c_MAC[0]																												
0x0350	RESERVED(8)	RESERVED(3)				MGR	S-YMDhms																						
0x0360	TRK-001	TRK-002	TRK-003	TRK-004	TRK-005	TRK-006	TRK-007	TRK-008																					
	TRK-009	TRK-010	TRK-011	TRK-012	TRK-013	TRK-014	TRK-015	TRK-016																					
0x0660	TRK-393	TRK-394	TRK-395	TRK-396	TRK-397	TRK-398	TRK-399	TRK-400																					
0x0670	INF-S(14720)																												
0x3FFF	BLKID-TLO	RESERVED	MCODE		REVISION						RESERVED																		

C

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	INF	0X00	ID	0X00	SIZE	MCODE	C+L	RESERVED	DATA VARIABLE LENGTH							

FIG. 21

ATTRACK-3 DATA FILE

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F																																				
0x0000	BLKID-HDO	RESERVED	MCODE	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED																																					
0x0010	N1C+L	N2C+L	INF SIZE	T-PRT	T-SU																																															
0x0020	NM1-S(256)																																																			
NM2-S(512)																																																				
0x0310																																																				
0x0320	RESERVED(3)	EKI	EKB VERSION	E(Kslm, Kcon)																																																
0x0330	E(KEKn, Kcon)																																																			
0x0340	RESERVED(8)																																																			
0x0350	INF_seq#																																																			
0x0360	MG(D)SERIAL-nnn(Upper)	A																																																		
0x0370	CONNUM	YMDhms-S	YMDhms-E	XCC	CT	CC	CN																																													
0x0380	PRTSIZE	LT																																																		
0x0390	FNo																																																			
PRTKEY																																																				
RESERVED(8)																																																				
CONNUMO																																																				
RESERVED(0x0400)																																																				
0x3FFF	BLKID-HDD	RESERVED	MCODE	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED	RESERVED																																					
0x4000	BLKID-A3D	RESERVED	MCODE	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO																																					
0x4010	BLOCKSEED																																																			
0x4020	INITIALIZATION VECTOR																																																			
0x41A0	SU-000(NByte=384Byte)																																																			
0x4320	SU-001(NByte)																																																			
0x04A0	SU-002(NByte)																																																			
0x7DA0	SU-041(NByte)																																																			
0x7F20	RESERVED(NByte=208Byte)																																																			
0x7FF0	BLKID-A3D	RESERVED	MCODE	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO	CONNUMO																																					

FIG. 22

FIG. 23

0x0320	RESERVED(3)	EKI	EKB VERSION	E[Ksim, Kcon)				
0x0330		E(KEn, Kcon)		C_MAC[n]				
0x0340	RESERVED(8)			INF_seq#	A	L	T	
0x0350	MG(D)SERIAL-mm(UPPER)				MG(D)SERIAL-mm(LOWER)			
0x0360	CONNUM	YMDhms-S	YMDhms-E	XCC	CT	CC	CN	

FIG. 24

Bit7 : ATRAC3 Mode 0 : Dual 1 : Joint

Bits 6, 5, 4: N OF 3-Bit CORRESPONDS TO MODE VALUE

N	MODE	TIME	TRANSFER RATE	SU (SOUND UNIT)	Byte
7	HQ	47min	176kbps	31SU	512
6		58min	146kbps	38SU	424
5	EX	64min	132kbps	42SU	384
4	SP	81min	105kbps	53SU	304
3		90min	94kbps	59SU	272
2	LP	128min	66kbps	84SU	192
1	MONO	181min	47kbps	119SU	136
0	MONO	258min	33kbps	169SU	96

Bit3 : RESERVED

Bit2 : DATA DISTINCTION 0 : AUDIO 1 : OTHERS

Bit1 : REPRODUCED SKIP 0 : NORMAL REPRODUCTION 1 : SKIP

Bit0 : EMPHASIS 0 : OFF 1 : ON(50/15 μ SECCOND)

FIG. 25

HCMS

Bit7 : COPY APPROVAL	0 : COPY INHIBITED	1 : COPY APPROVED
Bit6 : GENERATION (VERSION)	0 : ORIGINAL	1 : BEYOND THE FIRST GENERATION
Bit5-4 : CONTROL IN RELATION TO HIGH-SPEED DIGITAL COPYING OPERATION	00 : COPY INHIBITED	01 : COPY FOR THE FIRST GENERATION
	10 : COPY APPROVED	CHILD WHO IMPLEMENTED COPYING OF THE FIRST GENERATION IS INHIBITED FROM EXECUTING FURTHER COPYING OPERATION
Bit3-2 : MAGIC GATE AUTHENTICATION LEVEL	00: LEVEL10(Non-MG)	01 : LEVEL 1
	02: LEVEL12	11 : RESERVED
	02: LEVEL10	THOSE LEVELS OTHER THAN 10 CAN NOT BE DIVIDED NOR COMBINED
Bit1, 0 : RESERVED		

FIG. 26

0x0370	PRTSIZE	PRTKEY	RESERVED (8)
0x0380	CONNUMO	PRTSIZE(0x0388)	PRTKEY
0x0390	RESERVED (8)	CONNUMO	

FIG. 27

0x4000	BLKID-A3D	RESERVED	MCODE	CONNUMO	BLOCK SERIAL
0x4010	BLOCKSEED				INITIALIZATION VECTOR
0x4020	SU-000(NByte=384Byte)				

FIG. 28

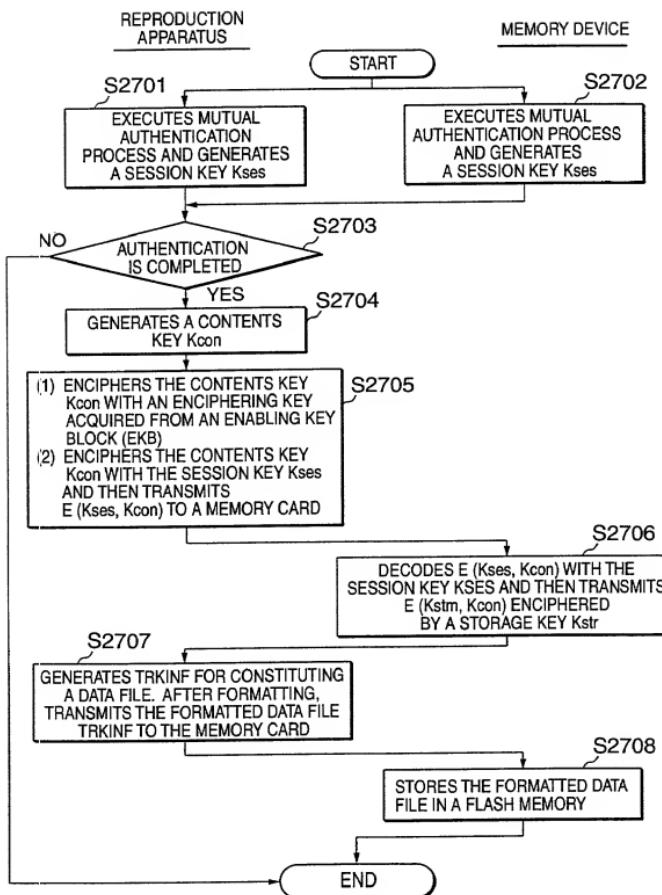


FIG. 29

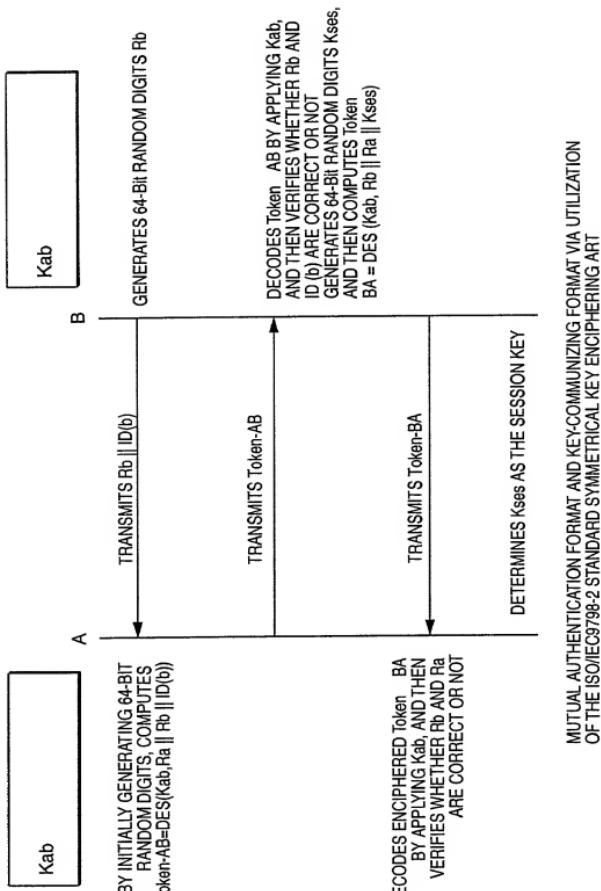


FIG. 30

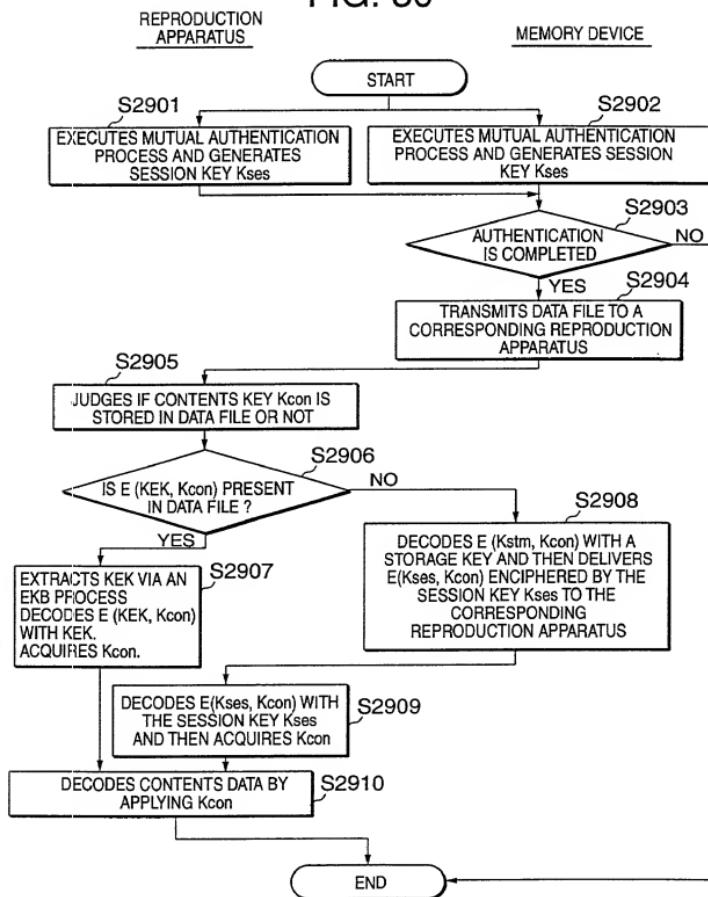


FIG. 31

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x0000	BLKID-EKB	RESERVED	MCODE	RESERVED(8)	LKF	LINK COUNT										
0x0010	RESERVED(8)					RESERVED(8)										
0x0020	VERSION	EA	RESERVED			KEK1										
0x0030			KEK2			E(VERSION)										
0x0040	SIZE OF TAG PART	SIZE OF KEY PART	SIZE OF SIGN PART													
0x0050				TAG PART {{X,O,O}, {X,1,1},.....}												
				FILL TO 64Bit ALIGNMENT												
														KEY PART		
															SIGNATURE	

FIG. 32

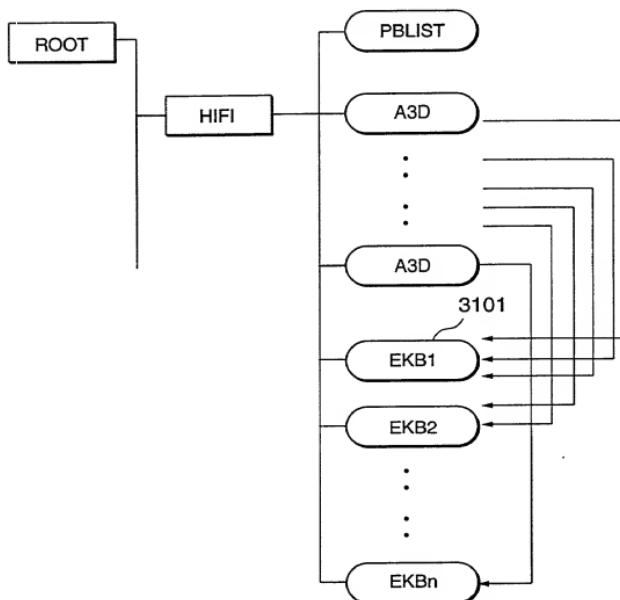


FIG. 33

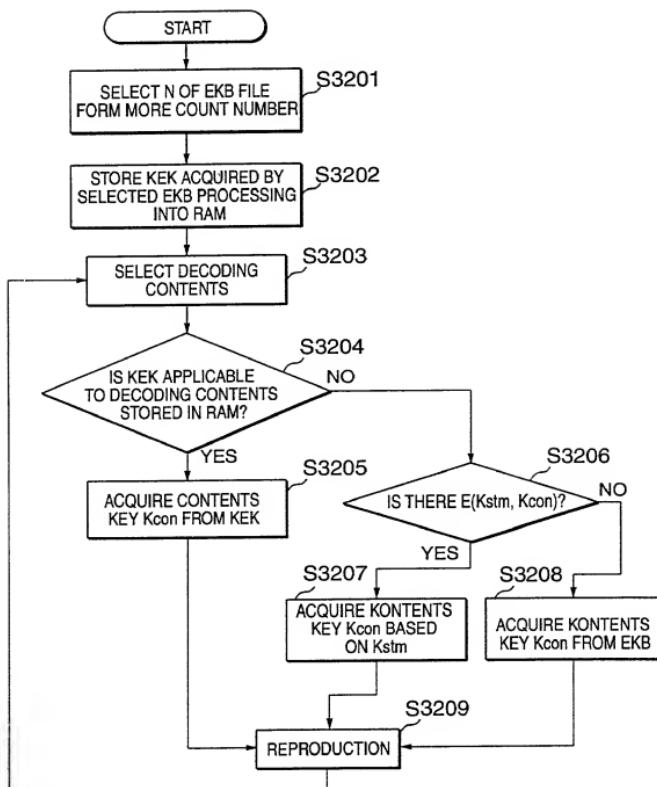


FIG. 34

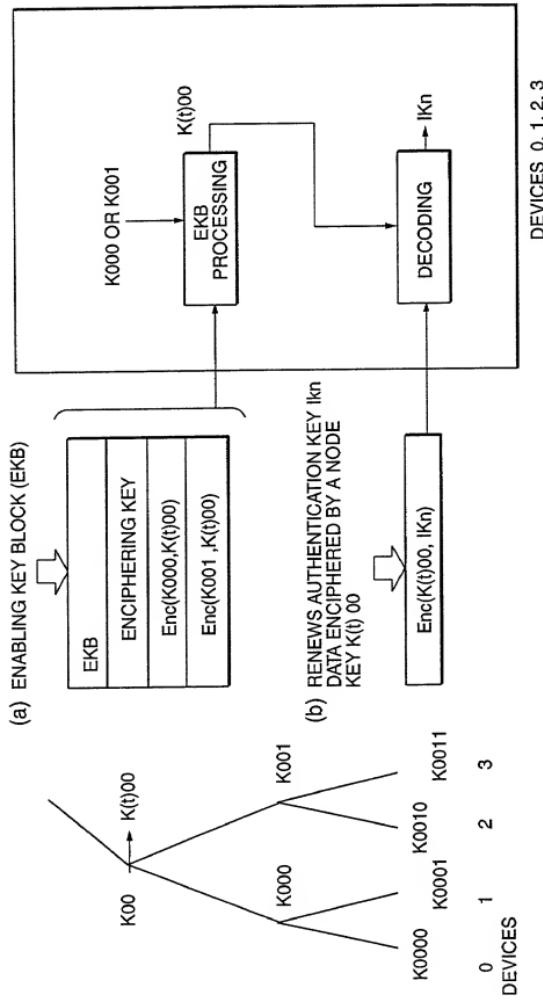


FIG. 35

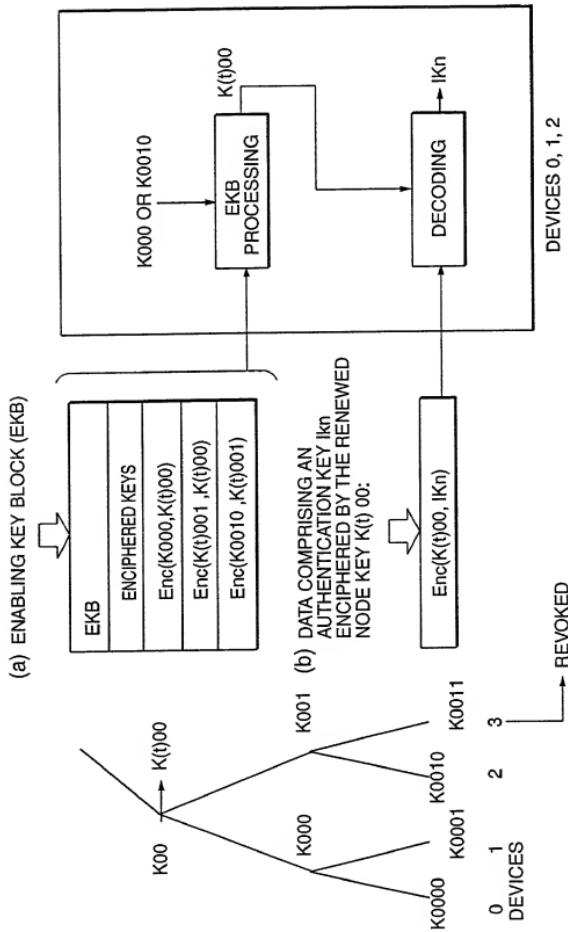


FIG. 36

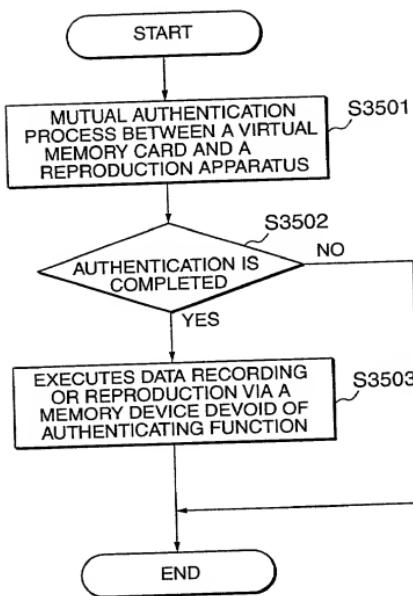
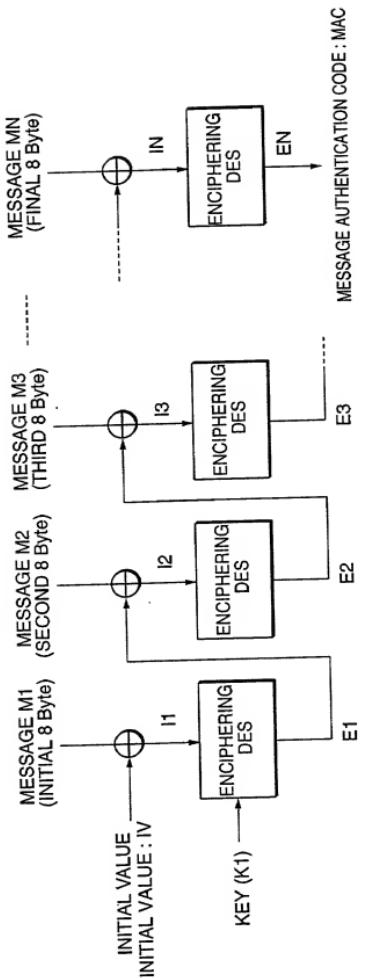


FIG. 37



⊕ EXCLUSIVE OR PROCESS (8 Bytes UNIT)

FIG. 38

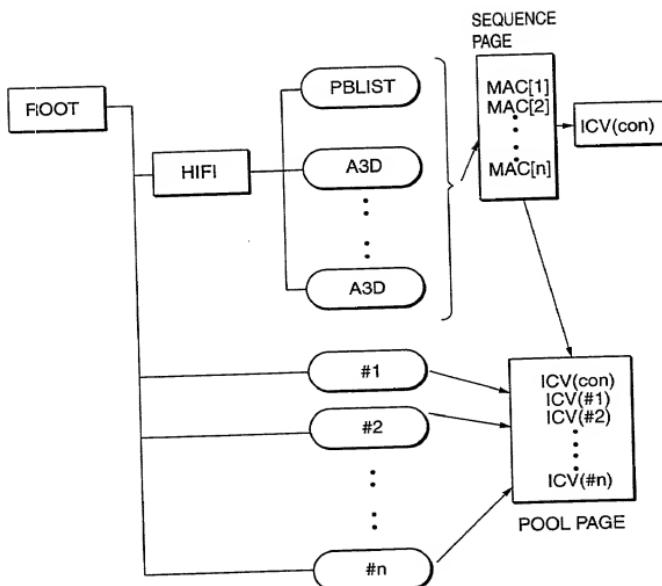
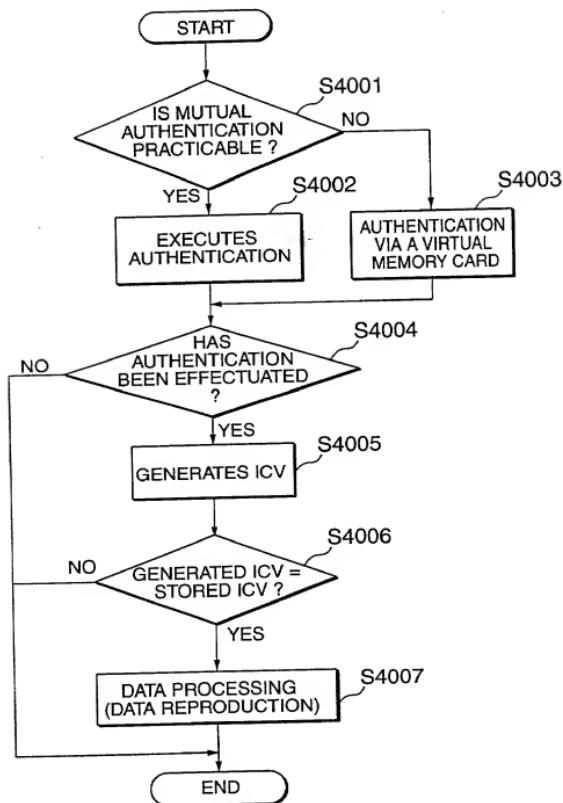


FIG. 39

FIG. 40

FIG. 41



TOP SECRET//SI//REL TO USA, FRA, GBR

FIG. 42

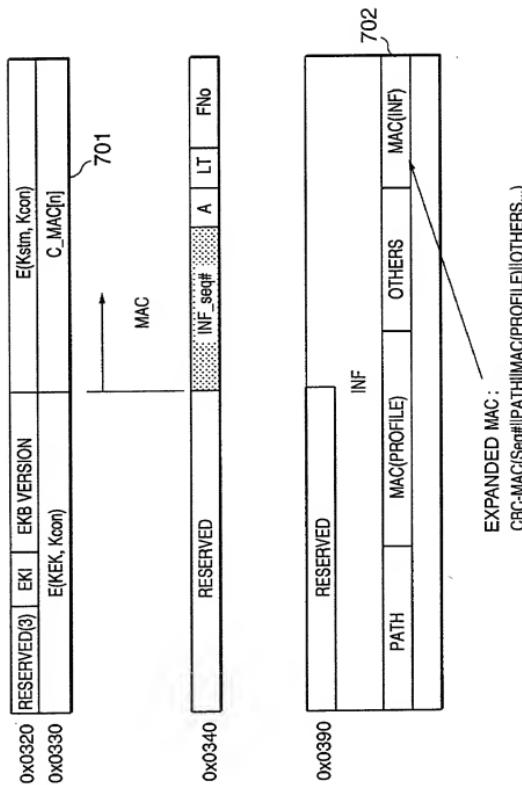


FIG. 4.3

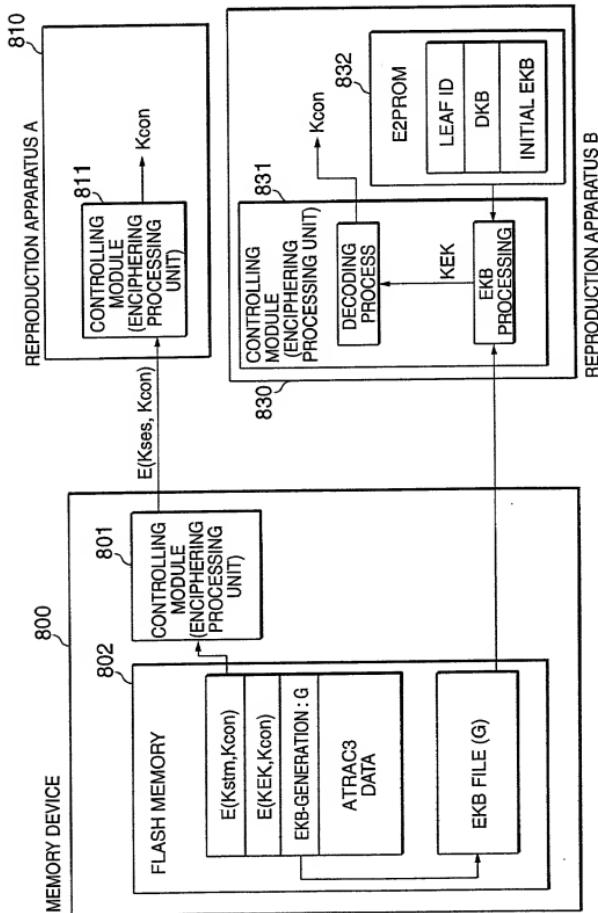


FIG. 44

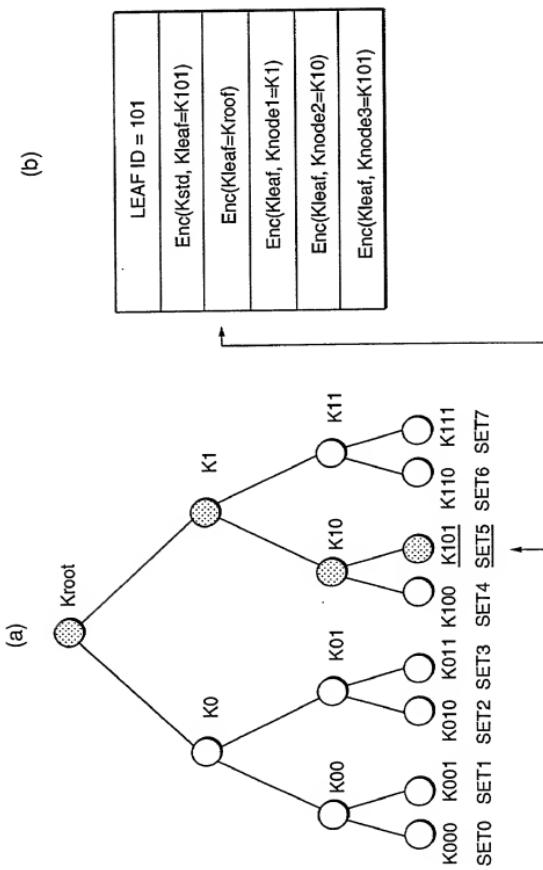


FIG. 45

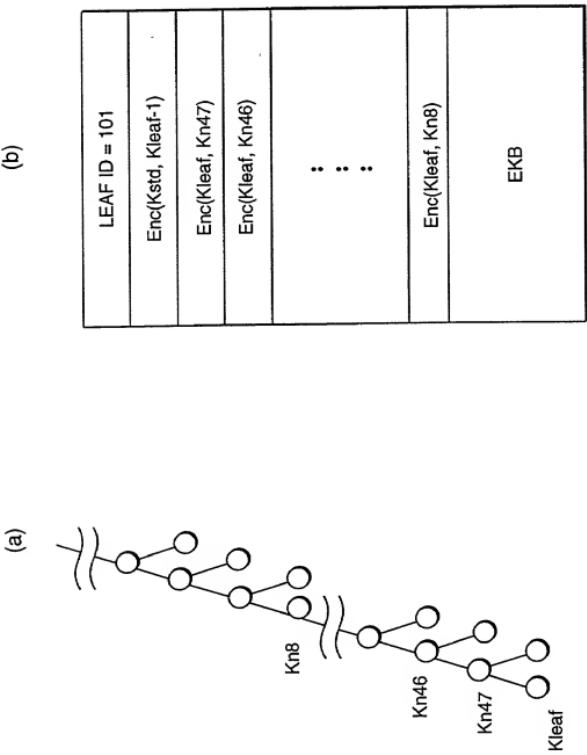


FIG. 46

